UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/750,511	12/27/2000	Balas Natarajan Kausik	028410-0002 DIV	6911

20350 7590 11/04/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
SEAL, JAMES	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/750,511	KAUSIK, BALAS NATARAJAN	
	Examiner	Art Unit	
	James Seal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *98* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *98* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 06 July 2004.

2. Claim 98 is pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 98 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan US 5535276, and further in view of Johnson et. al. US 5815573 and Matyas et. al. US 5142578 A.

5. As per claim 98, the limitation of dividing an private exponent d of the public key cryptosystem into two portions $d = d_a * d_b$ where * indicates the method of splitting, is taught by Ganesan in U.S. 5535276 (see Column 2, lines 59--61). Ganesan is silent on the method by which the key is split, that is the star operation.

6. Johnson teaches breaking a key into two or more portions according to the bit position in the register 102 (Column 4, line 17). Note that as the bit positions in a register refer to a power of two increasing from right to left, Johnson by teaching breaking the number into portions according to lengths (or bit position in the registers 102) then Johnson teaches breaking up the key into portions according to least significant and most significant portions. Further Johnson teaches that the length R determines the strength of the key and is the least significant portion of the number

stored in register 102 (see Column 7, line 4-5). Further Johnson teaches storing the resulting keys in tables (Column 12, lines 32-34). Thus Johnson teaches using the least significant portion of the private key. One of ordinary skill in the art at the time the invention was made would have been motivated to modify the teachings of Ganesan d = d_a * d_b where * represents any kind of splitting of d with those of Johnson that recommends that * splitting according to most and least significant portion of the key d, because it involves only basic operations of the shift registers which are already part of the machine. The limitation of storing in a secure database is taught by Ganesan (Column 14, lines 33-34), but Genesan and Johnson are silent on encryption of only a portion of the key.

7. Matyas discloses the use of Secure key management employment key encrypt key (KEK) storage as the preferred way for secure key storage (Column 2, line 66-68 and Column 3, lines 1-18). He further teaches that some parts of the key, e.g., the public key may be stored in unencrypted form while other protions e.g., the private key are stored encrypted form (Column 8, lines 58-63). This he explains can be for efficiency as well as speed as the public key is never secret. One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teaching of Genesan/Johnson with those Matyas because encryption implies extra time and as P+Q isn't really involved in the security of the encryption system it would be a waste of time to encrypt it while R which determines the strength of the encryption system it would be desirable to encrypt it. Claim 98 is rejected.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Response to Arguments

Applicant's arguments filed 06 April 2004 have been fully considered but they are not persuasive. The applicant argues that te step of dividing an exponent of the private key into a most significant portion and a least significant portion is not disclosed or suggested in any of the cited references. The examiner disagrees. Clearly Ganesan teaches dividing the private exponent into two parts $d = d_a * d_b$ where d is the private Column 2, lines 60-61; lines 33-35; lines 41-42; and lines 59-62, where * denotes a method of dividing or splitting the user's private key Column 2 , lines 60-61. Ganesan is silent on the method of splitting.

Johnson teaches dividing the key bits in a two portions $P \oplus Q$ and R (Column 7; line 20 and figure 1) to create a 112 bit key. Johnson further discloses that the length of the R value 108 determines the strength of the encryption (Column 7, line 4). Now the

bits stored in register 100 represent the coefficients of powers of two in binary, the right most bits referring to the lower powers and the left most bits referring to the largest powers. Thus Johnston teaches partitioning the key value according to least significant bits and most significant bits, and in particular the least significant portion providing the strength of the encryption system. Thus Johnson does teach dividing into a least significant portion and a most significant portion as he divides it according to the bits position in the register.

Matyas teaches storage of keys in encrypted form and in particular teaches the encryption of only those parts which carry a secret. Johnson teaches that the least significant portion R determines the strength of the encryption system while the part P +Q play no part in the strength of the algorithm. Hence according to Matyas teaching R should be encrypted but P + Q does not need to be.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JWS

James Seal
AU 2135
31 October 2004

KIM VU
PRIMARY PATENT EXAMINER
TECHNOLOGY CENTER 2100